

1. Let p be an odd prime and let d be a divisor of $p - 1$, it is known that the congruence $a^d \equiv 1 \pmod{p}$ has exactly d distinct solutions. Let a_1, a_2, \dots, a_d those solutions. Prove that $\sum_{i=1}^d a_i^n \equiv c_n \cdot d \pmod{p}$ where $c_n = 1$ if n is divisible by d and 0 otherwise.

Solution. We can prove that:

$$\left(\sum_{i=1}^d a_i^n\right) \left(\sum_{i=1}^d a_i^n - d\right) \equiv 0 \pmod{p}$$

Let $1 \leq i \leq d$, it is easy to prove that the remainders modulo p of the numbers $a_1 \cdot a_i, a_2 \cdot a_i, a_3 \cdot a_i, \dots, a_d \cdot a_i$ are all different and that satisfy $r^d - 1 \equiv 0 \pmod{p}$. Hence they are just $a_1, a_2, a_3, \dots, a_d$ in some order. The result follows by summing and using the binomial theorem. Therefore: $\sum_{i=1}^d a_i^n \equiv c_n \cdot d \pmod{p}$ where c_n is 0 or 1. On the other hand :

$$\left(\sum_{i=1}^d a_i^1 + \sum_{i=1}^d a_i^2 + \dots + \sum_{i=1}^d a_i^{d-1}\right) \equiv 0 \pmod{p}$$

We can rearrange the terms forming geometric progressions (we may assume $a_1 = 1$, since $1^d \equiv 1 \pmod{p}$) and then use the fact that $a_i^d \equiv 1 \pmod{p}$. Hence we have that: $(c_1 + c_2 + \dots + c_{d-1})d$ is divisible by p , d is relatively prime to p so the only possible value of $(c_1 + c_2 + \dots + c_{d-1})$ is zero, since otherwise it could not be divisible by p . Therefore we may deduce that $c_1 = c_2 = \dots = c_{d-1} = 0$ and $\sum_{i=1}^d a_i^n$ is divisible by p for $n = 1, 2, \dots, d - 1$.

$$\sum_{i=1}^d a_i^{n+d} \equiv \sum_{i=1}^d a_i^n \pmod{p}$$

On the other hand, it is easy to prove that for n multiple of d : $\sum_{k=1}^d k^n$ is of the form $p \cdot m + d$. Hence $\sum_{i=1}^d a_i^n \equiv c_n \cdot d \pmod{p}$ where $c_n = 1$ if n is divisible by d and 0 otherwise.